Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - **Adobe Acrobat and Reader File Discovery (Updated)**
  - Crob FTP Server Buffer Overflow Vulnerabilities
  - Doug Luxem Liberum Help Desk "id" SQL Injection Vulnerability
  - E-POST SPA-PRO Mail @Solomon IMAP Directory Traversal and Buffer Overflow
  - **GlobalSCAPE Secure FTP Server Buffer Overflow Lets Remote Users Execute Arbitrary Code (Updated)**
  - JiRo's Upload System Input Validation Vulnerability Lets Remote Users Inject SQL Commands
  - Kaspersky Anti-Virus Klif.Sys Privilege Escalation Vulnerability
  - livingmailing Input Validation Hole Lets Remote Users Inject SQL Commands
  - Microsoft Windows Remote Desktop Protocol Private Key Disclosure
  - Microsoft ISA Server in SecureNAT Configuration Denial of Service
  - NEXTWEB (i)Site Discloses Database and Passwords to Remote Users and Permits SQL Injection
  - **Nortel Contivity VPN Client Password Disclosure Vulnerability (Updated)**
  - Perception LiteWeb Protected File Access Vulnerability
  - **RSA Authentication Agent for Web for IIS Cross-Site Scripting Vulnerability (Updated)**
  - software602 602LAN SUITE HTML Log File Processing Flaw Lets Remote Users Hide Log Entries
  - WWWeb Concepts Events System Input Validation Vulnerability
- UNIX / Linux Operating Systems
  - Adrian Pascalau GIPTables Firewall Insecure Temporary File Creation
  - **Apple QuickTime Quartz Composer File Information Disclosure (Updated)**
  - **Bzip2 Remote Denial of Service (Updated)**
  - **BZip2 File Permission Modification (Updated)**
  - **Cyrus SASL Buffer Overflow & Input Validation (Updated)**
  - **Ethereal Multiple Remote Protocol Dissector Vulnerabilities (Updated)**
  - Everybuddy Insecure Temporary File Creation
  - **FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow (Updated)**
  - FUSE Information Disclosure
  - **gFTP Remote Directory Traversal (Updated)**
  - **GNU GZip Directory Traversal (Updated)**
  - **GNU Mailutils Buffer Overflow and Format String Bugs Let Remote Users Execute Arbitrary Code (Updated)**
  - **GNU GZip File Permission Modification (Updated)**
  - **GnuTLS Padding Validation Remote Denial of Service (Updated)**
  - **Gzip Zgrep Arbitrary Command Execution (Updated)**
  - **HP-UX ICMP PMTUD Remote Denial of Service (Updated)**
  - **LibEXIF Library EXIF Tag Structure Validation (Updated)**
  - **LibTIFF TIFFOpen Remote Buffer Overflow (Updated)**
  - **Marc Lehmann Convert-UUlib Perl Module Buffer Overflow (Updated)**
  - Mortiforo Access Control
  - **Multiple Vendors FreeBSD Hyper-Threading Technology Support Information Disclosure (Updated)**
  - GNU Binutils Binary File Descriptor Library Integer Overflow
  - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
  - **Multiple Vendors GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service (Updated)**
  - GNU Mailutils Authentication Module SQL Injection
  - **ImageMagick & GraphicsMagick XWD Decoder Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Moxa Char Driver Buffer Overflows (Updated)**
  - **Multiple Vendors Linux Kernel ELF Core Dump Buffer Overflow (Updated)**
  - Multiple Vendors Linux Kernel Radionet Open Source Environment (ROSE) ndigis Input Validation
  - **Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index (Updated)**
  - **Multiple Vendors Linux Kernel PROC Filesystem Local Information Disclosure (Updated)**
  - **Multiple Vendors Linux Kernel Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel EXT2 File System Information Leak (Updated)**
  - **Multiple Vendors Linux Kernel Terminal Locking Race Condition (Updated)**
  - **Multiple Vendors NASM IEEE_PUTASCII Remote Buffer Overflow (Updated)**
  - **Multiple Vendors Qpopper Multiple Insecure File Handling (Updated)**
  - **PostgreSQL Remote Denial of Service & Arbitrary Code Execution (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Adobe Adobe Reader 7.0 and earlier Adobe Acrobat 7.0 and earlier	The Acrobat web control in Adobe Acrobat and Acrobat Reader 7.0 and earlier, when used with Internet Explorer, allows remote malicious users to determine the existence of arbitrary files via the LoadFile ActiveX method. This is a separate issue from CAN-2005-1347. Updates available: http://www.adobe.com/support/techdocs/331465.html Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat and Reader File Discovery CAN-2005-0035	Low	Adobe Advisory, Document 331465, April 1, 2005 **US-CERT VU#250037**
Crob Software Studio Crob FTP Server 3.6.1	Multiple vulnerabilities have been reported that could let remote malicious users execute arbitrary code. This is due to a boundary error in the argument handling in the 'STOR' and 'RMD' commands and a boundary error in the 'LIST' or 'NLST' commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Crob FTP Server Buffer Overflow Vulnerabilities CAN-2005-1873	High	LSS Security Advisory #LSS-2005-06-06, June 6, 2005
Doug Luxem Liberum Help Desk 0.97.3	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. Input passed to the 'id' parameter isn't properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Doug Luxem Liberum Help Desk "id" SQL Injection Vulnerability CAN-2005-1839	High	Secunia SA15593, June 3, 2005
E-POST Corporation SPA-PRO Mail @Solomon 4.x	Two vulnerabilities have been reported that could let remote malicious users access sensitive information or execute arbitrary code. This is due to missing input validation in the IMAP service and a boundary error in the IMAP service. Update the SPA-IMAP4S component to version 4.05. A Proof of Concept exploit has been published.	E-POST SPA-PRO Mail @Solomon IMAP Directory Traversal and Buffer Overflow CAN-2005-1902 CAN-2005-1903	High	SIG^2 Vulnerability Research Advisory, June 2, 2005
GlobalSCAPE Secure FTP Server 3.0.2	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code on the target system. The remote user can overwrite the EIP (and SEH) registers with an arbitrary address. The vendor has reportedly issued a fix: http://www.cuteftp.com/gsftps/ **Another Proof of Concept exploit script has been published.**	GlobalSCAPE Secure FTP Server Buffer Overflow Lets Remote Users Execute Arbitrary Code CAN-2005-1415	High	Security Focus Bugtraq ID 13454, May 2, 2005 **Security Focus, 13454, June 2, 2005**
JiRo's JiRo's Upload System v1	A vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'login.asp' script does not properly validate user-supplied input in the 'password' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	JiRo's Upload System Input Validation Vulnerability Lets Remote Users Inject SQL Commands CAN-2005-1904	High	Security Tracker Alert,1014086, June 1, 2005
Kaspersky Labs Kaspersky Anti-Virus for Microsoft Windows 2000, versions 5.0.227, 5.0.228, and 5.0.335	A privilege escalation vulnerability has been reported due to a problem in the Kaspersky kernel driver 'klif.sys.' This issue may ultimately result in the execution of attacker-supplied code in the context of the system kernel (ring-0). No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Kaspersky Anti-Virus Klif.Sys Privilege Escalation Vulnerability CAN-2005-1905	High	Security Focus, Bugtraq ID: 13878, June 6, 2005
livingcolor livingmailing 1.3	A vulnerability has been reported that could let a remote malicious user can inject SQL commands. The 'login.asp' script does not properly validate user-supplied input in the 'password' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	livingmailing Input Validation Hole Lets Remote Users Inject SQL Commands CAN-2005-1906	High	Security Tracker Alert, 1014087, June 1, 2005
Microsoft Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Microsoft Windows Server 2003 Web Edition, Windows XP Home Edition, Windows XP Professional	A security issue has been reported that could let a remote malicious user conduct Man-in-the-Middle attacks. The problem is that the private key used for signing a terminal server's public key is hard-coded into the mstlsapi.dll library. This can be exploited to calculate a valid signature. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows Remote Desktop Protocol Private Key Disclosure CAN-2005-1794	Medium	Secunia SA15605, June 6, 2005

Microsoft Microsoft Internet Security and Acceleration (ISA) Server prior than 3.0.1200.411	A vulnerability has been reported in the firewall service that could let a remote malicious user cause a Denial of Service. If client computers are configured as SecureNAT clients and generate heavy network traffic via the firewall, the 'Wspsrv.exe' service may crash. An update is available at: http://support.microsoft.com/kb/894864/EN-US/ Currently we are not aware of any exploits for this vulnerability.	Microsoft ISA Server in SecureNAT Configuration Denial of Service CAN-2005-1907	Low	Microsoft Knowledge base Article ID : 894864, May 31, 2005
NEXTWEB (i)site	Multiple vulnerabilities have been reported that could let a remote malicious user inject SQL commands or download the application database and obtain the administrative password. The 'admin/login.asp' script does not properly validate user-supplied input in the 'password' parameter. Also, the application database ('users.mdb') is stored by default in the web document directory. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	NEXTWEB (i)Site Discloses Database and Passwords to Remote Users and Permits SQL Injection CAN-2005-1834 CAN-2005-1835 CAN-2005-1836	High	Zone-H Security Labs, ZH2005-13SA, June1, 2005
Nortel Nortel Contivity VPN Client 5.01	A vulnerability has been reported that could let a local malicious user obtain the password. This is because of the way the VPN client software stores the VPN password in process memory. A local user with access to the 'Extranet.exe' process memory can recover the user or group password. **Update information available at:** **http://www116.nortelnetworks.com/pub/repository/CLARIFY/DOCUMENT/2005/21/019126-02.pdf** A Proof of Concept exploit has been published.	Nortel Contivity VPN Client Password Disclosure Vulnerability CAN-2005-0844	High	Security Tracker Alert, 1013512, March 22, 2005 **Nortel Security Bulletin, May 27, 2005**
Perception LiteWeb 2.5	A vulnerability has been reported that could let remote malicious users bypass certain security restrictions. The vulnerability is caused due to an access control error allowing unauthorized access to password-protected files. The vulnerability will reportedly be fixed in the next version. A Proof of Concept exploit has been published.	Perception LiteWeb Protected File Access Vulnerability CAN-2005-1908	Medium	Secunia SA15592, June 3, 2005
RSA Security RSA Authentication Agent for Web for IIS 5.2	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to input validation errors in the "postdata" parameter in "/WebID/IISWebAgentIF.dll." Update to version 5.3: http://www.rsasecurity.com/node.asp?id=2807&node_id= A Proof of Concept exploit has been published.	RSA Authentication Agent for Web for IIS Cross-Site Scripting Vulnerability CAN-2005-1118	High	Secunia SA14954, April 15, 2005 **US-CERT Note VU#366372**
software602 602LAN SUITE 2004	A vulnerability has been reported that could let a remote malicious user alter the administrator's view of the log files. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	software602 602LAN SUITE HTML Log File Processing Flaw Lets Remote Users Hide Log Entries CAN-2005-1909	Medium	Security Tracker Alert, 1014105, June 6, 2005
WWWeb Concepts Events System 1.0	A vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'login.asp' script does not properly validate user-supplied input in the 'password' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	WWWeb Concepts Events System Input Validation Vulnerability CAN-2005-1910	High	Security Tracker Alert, 1014104, June 5, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adrian Pascalau GIPTables Firewall 1.0, 1.1	A vulnerability has been reported due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files or cause a Denial of Service by manipulating the IP addresses inside the temporary file. No workaround or patch available at time of publishing. There is no exploit code required.	GIPTables Firewall Insecure Temporary File Creation CAN-2005-1878	Medium	Securiteam, June 6, 2005

Apple QuickTime Player 7.0	A vulnerability has been reported in the QuickTime Web plugin because Quartz Composer compositions that are embedded in '.mov' files can access system information, which could let a remote malicious user obtain sensitive information. **Upgrade available at:** **http://www.apple.com/quicktime/download/mac.html** A Proof of Concept exploit has been published.	Apple QuickTime Quartz Composer File Information Disclosure CAN-2005-1579	Medium	Security Tracker Alert, 1013961, May 12, 2005 **Apple Security Advisory, APPLE-SA-2005-05-31, May 31, 2005**
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when the application processes malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 **Turbolinux Security Advisory , TLSA-2005-60, June 1, 2005**
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/b/bzip2/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 **Debian Security Advisory, DSA 730-1, May 27, 2005** **Turbolinux Security Advisory , TLSA-2005-60, June 1, 2005**
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-sasl/ Conectiva: ftp://atualizacoes.conectiva.com.br/ OpenPGK: ftp ftp.openpkg.org FedoraLegacy: http://download.fedoralegacy.	Cyrus SASL Buffer Overflow & Input Validation CAN-2004-0884 CAN-2005-0373	High	Security Tracker Alert ID: 1011568, October 7, 2004 Debian Security Advisories DSA 563-2, 563-3, & 568-1, October 12, 14, & 16, 2004 Conectiva Linux Security Announcement, CLA-2004:889, November 11, 2004 OpenPKG Security Advisory, OpenPKG Security Advisory, January 28, 2005 Fedora Legacy Update Advisory, FLSA:2137, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Announcement, SUSE-SA:2005:013, March 3, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:054, March 16, 2005 Apple Security Update, APPLE-SA-2005-03-21,

	org/redhat/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Apple: http://www.apple.com/support/downloads/securityupdate2005003client.html **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000959** Currently we are not aware of any exploits for these vulnerabilities.			March 21, 2005 **Conectiva Security Advisory, CLSA-2005:959, June 2, 2005**
Ethereal Group Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509. Upgrades available at: http://www.ethereal.com/distribution/ethereal-0.10.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-03.xml Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-427.html **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000963** **SuSE:** **ftp://ftp.suse.com/pub/suse/** An exploit script has been published.	Ethereal Multiple Remote Protocol Dissector Vulnerabilities CAN-2005-1456 CAN-2005-1457 CAN-2005-1458 CAN-2005-1459 CAN-2005-1460 CAN-2005-1461 CAN-2005-1462 CAN-2005-1463 CAN-2005-1464 CAN-2005-1465 CAN-2005-1466 CAN-2005-1467 CAN-2005-1468 CAN-2005-1469 CAN-2005-1470	High	Ethereal Security Advisory, enpa-sa-00019, May 4, 2005 Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:083, May 11, 2005 RedHat Security Advisory, RHSA-2005:427-05, May 24, 2005 **Conectiva Security Advisory, CLSA-2005:963, June 6, 2005** **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
Everybuddy Everybuddy 0.4.3 & prior	A vulnerability has been reported because the 'modules/utility/autotrans.c' file creates temporary files insecurely, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Everybuddy Insecure Temporary File Creation CAN-2005-1880	Medium	Security Tracker Alert, 1014110, June 6, 2005
FreeRADIUS Server Project FreeRADIUS 1.0.2	Two vulnerabilities have been reported: a vulnerability was reported in the 'radius_xlat()' function call due to insufficient validation, which could let a remote malicious user execute arbitrary SQL code; and a buffer overflow vulnerability was reported in the 'sql_escape_func()' function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200505-13.xml **SuSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow CAN-2005-1454 CAN-2005-1455	High	Security Tracker Alert ID: 1013909, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-13, May 17, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
FUSE FUSE 2.x	A vulnerability has been reported because certain memory is not correctly cleared before returned to users, which could let a malicious user obtain sensitive information. Update available at: http://sourceforge.net/project/showfiles.php?group_id=121684 A Proof of Concept exploit script has been published.	FUSE Information Disclosure CAN-2005-1858	Medium	Secunia Advisory, SA15561, June 3, 2005

gFTP gFTP 0.1, 0.2, 0.21, 1.0, 1.1-1.13, 2.0-2.0.17	A Directory Traversal vulnerability exists due to insufficient sanitization of input, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.gftp.org/gftp-2.0.18.tar.gz Debian: http://security.debian.org/pool/updates/main/g/gftp/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-27.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000957** There is no exploit code required.	gFTP Remote Directory Traversal CAN-2005-0372	Medium	Security Focus, February 14, 2005 Debian Security Advisory, DSA 686-1, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 Gentoo Linux Security Advisory, GLSA 200502-27, February 19, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:050, March 4, 2005 **Conectiva Security Advisory, CLSA-2005:957, May 31, 2005**
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 **Turbolinux Security Advisory , TLSA-2005-59, June 1, 2005**
GNU Mailutils 0.5, 0.6	Multiple vulnerabilities have been reported that could let a remote malicious user execute arbitrary code or cause a Denial of Service. These vulnerabilities are due to a buffer overflow in the 'header_get_field_name()' function in 'mailbox/header.c'; an integer overflow in the 'fetch_io()' function; an input validation error in the imap4d server in the FETCH command; and a format string flaw in the imap4d server. A fixed version (0.6.90) is available at: ftp://alpha.gnu.org/gnu/mailutils/mailutils-0.6.90.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-20.xml **Debian:** **http://security.debian.org/pool/updates/main/m/mailutils/** Proofs of Concept exploits have been published.	GNU Mailutils Buffer Overflow and Format String Bugs Let Remote Users Execute Arbitrary Code CAN-2005-1520 CAN-2005-1521 CAN-2005-1522 CAN-2005-1523	High	iDEFENSE Security Advisory 05.25.05 Gentoo Linux Security Advisory, GLSA 200505-20, May 27, 2005 **Debian Security Advisory, DSA 732-1, June 3, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux

	Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.			Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 **Turbolinux Security Advisory , TLSA-2005-59, June 1, 2005**
GnuTLS GnuTLS 1.2 prior to 1.2.3; 1.0 prior to 1.0.25	A remote Denial of Service vulnerability has been reported due to insufficient validation of padding bytes in 'lib/gnutils_cipher.c.' Updates available at: http://www.gnu.org/software/gnutls/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-04.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gnutls10/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-430.html** Currently we are not aware of any exploits for this vulnerability.	GnuTLS Padding Validation Remote Denial of Service CAN-2005-1431	Low	Security Tracker Alert, 1013861, May 2, 2005 Fedora Update Notification, FEDORA-2005-362, May 5, 2005 Gentoo Linux Security Advisory, GLSA 200505-04, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:084, May 12, 2005 Ubuntu Security Notice, USN-126-1, May 13, 2005 **RedHat Security Advisory, RHSA-2005:430-05, June 1, 2005**
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 Mandriva: http://www.mandriva.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 **Turbolinux Security Advisory , TLSA-2005-59, June 1, 2005**
Hewlett Packard Company HP-UX B.11.23, B.11.22, B.11.11, B.11.04, B.11.00	A remote Denial of Service vulnerability has been reported in the Path MTU Discovery (PMTUD) functionality that is supported in the ICMP protocol. Patches available at: http://www1.itrc.hp.com/service/cki/docDisplay.do?docId= HPSBUX01137 **Revision 2: The binary files of HPSBUX01164 will resolve the issue for the core TCP/IP in B.11.11, B.11.22, and B.11.23.** **The binary files of HPSBUX01164 will resolve NOT resolve the issue for IPSec. B.11.00 and B.11.04 are NOT vulnerable.** **The recommended workaround is to modify /etc/rc.config.d/nddconf and reboot.** Currently we are not aware of any exploits for this vulnerability.	HP-UX ICMP PMTUD Remote Denial of Service CAN-2005-1192	Low	Hewlett Packard Company Security Advisory, HPSBUX01137, April 24, 2005 Hewlett Packard Company Security Advisory, HPSBUX01137: SSRT5954 rev.1, May 25, 2005 **Hewlett Packard Company Security Advisory, HPSBUX01137: SSRT5954 rev.2, June 1, 2005**
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/	LibEXIF Library EXIF Tag Structure Validation	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update

	pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-17.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-300.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/libe/libexif/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Peachtree: http://peachtree.burdell.org/updates/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000960** Currently we are not aware of any exploits for this vulnerability.	CAN-2005-0664		Notifications, FEDORA-2005-199 & 200, March 8, 2005 Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005 RedHat Security Advisory, RHSA-2005:300-08, March 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:064, March 31, 2005 Debian Security Advisory, DSA 709-1, April 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005 Peachtree Linux Security Notice, PLSN-0006, April 22, 2005 **Conectiva Security Advisory, CLSA-2005:960, June 2, 2005**
LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6.0, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability has been reported in the 'TIFFOpen()' function when opening malformed TIFF files, which could let a remote malicious user execute arbitrary code. Patches available at: http://bugzilla.remotesensing.org/attachment.cgi?id=238 Gentoo: http://security.gentoo.org/glsa/glsa-200505-07.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tiff/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	LibTIFF TIFFOpen Remote Buffer Overflow CAN-2005-1544 CAN-2005-1472	High	Gentoo Linux Security Advisory, GLSA 200505-07, May 10, 2005 Ubuntu Security Notice, USN-130-1, May 19, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
Marc Lehmann Convert-UUlib 1.50	A buffer overflow vulnerability has been reported in the Convert::UUlib module for Perl due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://search.cpan.org/dist/Convert-UUlib/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-26.xml Debian: http://security.debian.org/pool/updates/main/libc/libconvert-uulib-perl/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Convert-UUlib Perl Module Buffer Overflow CAN-2005-1349	High	Gentoo Linux Security Advisory, GLSA 200504-26, April 26, 2005 Secunia Advisory, SA15130, April 27, 2005 Debian Security Advisory, DSA 727-1, May 20, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
Mortiforo Mortiforo prior to 0.9.1	A vulnerability has been reported because a remote malicious user can access private forums without permission. Update available at: http://mortiforo.sourceforge.net/download.html There is no exploit code required.	Mortiforo Access Control CAN-2005-1890	Medium	Security Tracker Alert, 1014120, June 7, 2005

Multiple Vendors FreeBSD 5.4 & prior	A vulnerability was reported in FreeBSD when using Hyper-Threading Technology due to a design error, which could let a malicious user obtain sensitive information and possibly elevated privileges. Patches and updates available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:09.htt.asc SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.24 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-476.html** **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101739-1** **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	**Multiple Vendor** FreeBSD Hyper-Threading Technology Support Information Disclosure CAN-2005-0109	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:09, May 13, 2005 SCO Security Advisory, SCOSA-2005.24, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 US-CERT VU#911878 **RedHat Security Advisory, RHSA-2005:476-08, June 1, 2005** **Sun(sm) Alert Notification, 101739, June 1, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:096, June 7, 2005**
Multiple Vendors GNU Binutils 2.14, 2.15 ; Gentoo Linux	A vulnerability was reported in the GNU Binutils Binary File Descriptor Library due to an integer overflow, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200506-01.xml Currently we are not aware of any exploits for this vulnerability.	GNU Binutils Binary File Descriptor Library Integer Overflow CAN-2005-1704	High	Gentoo Linux Security Advisory, GLSA 200506-01, June 1, 2005
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**

Multiple Vendors GNOME GdkPixbuf 0.22 GTK GTK+ 2.4.14 RedHat Fedora Core3 RedHat Fedora Core2	A remote Denial of Service vulnerability has been reported due to a double free error in the BMP loader. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-344.html http://rhn.redhat.com/errata/RHSA-2005-343.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: ftp://patches.sgi.com/support/free/security/advisories/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000958** Currently we are not aware of any exploits for this vulnerability.	GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service CAN-2005-0891	Low	Fedora Update Notifications, FEDORA-2005-265, 266, 267 & 268, March 30, 2005 RedHat Security Advisories, RHSA-2005:344-03 & RHSA-2005:343-03, April 1 & 4, 2005 Ubuntu Security Notice, USN-108-1 April 05, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:068 & 069, April 8, 2005 SGI Security Advisory, 20050403-01-U, April 15, 2005 Turbolinux Security Advisory, TLSA-2005-57, May 16, 2005 **Conectiva Security Advisory, CLSA-2005:958, June 1, 2005**
Multiple Vendors GNU Mailutils 0.6.90, 0.6, 0.5	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Gentoo: http://security.gentoo.org/glsa/glsa-200506-02.xml There is no exploit code required.	GNU Mailutils Authentication Module SQL Injection CAN-2005-1824	High	Gentoo Linux Security Advisory, GLSA 200506-02, June 6, 2005
Multiple Vendors GraphicsMagick GraphicsMagick 1.0, 1.0.6, 1.1, 1.1.3-1.1.6; ImageMagick ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8, 5.5.3.2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0-6.0.8, 6.1-6.1.8, 6.2.0.7, 6.2 .0.4, 6.2-6.2.2	A remote Denial of Service vulnerability has been reported due to a failure to handle malformed XWD image files. Gentoo: http://security.gentoo.org/glsa/glsa-200505-16.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-480.html** Currently we are not aware of any exploits for this vulnerability.	ImageMagick & GraphicsMagick XWD Decoder Remote Denial of Service CAN-2005-1739	Low	Gentoo Linux Security Advisory, GLSA 200505-16, May 21, 2005 Ubuntu Security Notice, USN-132-1, May 23, 2005 Fedora Update Notification, FEDORA-2005-395, May 26, 2005 **RedHat Security Advisory, RHSA-2005:480-03, June 2, 2005**
Multiple Vendors Linux Kernel 2.2, 2.4, 2.6	Several buffer overflow vulnerabilities exist in 'drivers/char/moxa.c' due to insufficient validation of user-supplied inputs to the 'MoxaDriverIoctl(),' ' moxaloadbios(),' moxaloadcode(),' and 'moxaload320b()' functions, which could let a malicious user execute arbitrary code with root privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/l SUSE: ftp://ftp.SUSE.com/pub/SUSE **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Moxa Char Driver Buffer Overflows CAN-2005-0504	High	Security Tracker Alert, 1013273, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**

Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available at: http://kernel.org/ Trustix: http://www.trustix.org/ errata/2005/0022/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-472.html **Avaya:** **http://support.avaya.com/** **elmodocs2/security/ASA-2005-120_RHSA-2005-283_** **RHSA-2005-284_** **RHSA-2005-293_** **RHSA-2005-472.pdf** An exploit script has been published.	Linux Kernel ELF Core Dump Buffer Overflow CAN-2005-1263	High	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 **Avaya Security Advisory, ASA-2005-120, June 3, 2005**
Multiple Vendors Linux Kernel 2.4.x, 2.6 prior to 2.6.11.11	A vulnerability has been reported in the Linux kernel in the Radionet Open Source Environment (ROSE) implementation in the 'rose_rt_ioctl()' function due to insufficient validation of a new routes' ndigis argument. The impact was not specified. Updates available at: http://linux.bkbits.net:8080/ linux-2.4/cset@41e2cf515Tpixc VQ8g8HvQvCv9E6zA Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Radionet Open Source Environment (ROSE) ndigis Input Validation	Not Specified	Security Tracker Alert, 1014115, June 7,2005
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/ kernel/v2.4/testing/patch- 2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/ trustix/updates/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/ errata/RHSA-2005-283.html http://rhn.redhat.com/ errata/RHSA-2005-284.html Conectiva: ftp://atualizacoes.conectiva. com.br/ **FedoraLegacy:** **http://download.fedoralegacy.org/** **redhat/** A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005 :021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel /proc filesystem is susceptible to an information disclosure vulnerability. This issue is due to a race-condition allowing unauthorized access to potentially sensitive process information. This vulnerability may allow malicious local users to gain access to potentially sensitive	Multiple Vendors Linux Kernel PROC Filesystem Local Information	Medium	Ubuntu Security Notice USN-38-1 December 14, 2004

	environment variables in other users processes. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-293.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Disclosure CAN-2004-1058		Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 Turbolinux Security Announcement, February 28, 2005 **Avaya Security Advisory, ASA-2005-120, June 3, 2005** **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**

Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Trustix: http://http.trustix.org/pub/trustix/updates SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-283.html http://rhn.redhat.com/errata/RHSA-2005-284.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 **Avaya Security Advisory, ASA-2005-120, June 3, 2005** **Fedora Legacy Update Advisory, FLSA:152532, June 4, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-283.html http://rhn.redhat.com/errata/RHSA-2005-284.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-472.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Medium	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 **Avaya Security Advisory, ASA-2005-120, June 3, 2005** **FedoraLegacy: FLSA:152532, June 4, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1- 2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html Conectiva: ftp://atualizacoes.conectiva.com.br/	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 **Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005**

	FedoraLegacy: **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux Kernel versions except 2.6.9	A race condition vulnerability exists in the Linux Kernel terminal subsystem. This issue is related to terminal locking and is exposed when a remote malicious user connects to the computer through a PPP dialup port. When the remote user issues the switch from console to PPP, there is a small window of opportunity to send data that will trigger the vulnerability. This may cause a Denial of Service. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php FedoraLegacy: http://download.fedoralegacy.org/redhat/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Terminal Locking Race Condition CAN-2004-0814	Low	Security Focus, December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005 Turbolinux Security Announcement , February 28, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 **Avaya Security Advisory, ASA-2005-120, June 3, 2005**
Multiple Vendors NASM NASM 0.98.35, 0.98.38; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, r 2.1, Desktop 3.0, 4.0 RedHat Enterprise Linux WS 4, 3, 2.1 IA64, 2.1, ES 4, 3, 2.1 IA64, 2.1, AS 4, 3, 2.1 IA64, 2.1	A buffer overflow vulnerability has been reported in the 'ieee_putascii()' function, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-381.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/nasm/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	NASM IEEE_PUTASCII Remote Buffer Overflow CAN-2005-1194	High	RedHat Security Advisory, RHSA-2005:381-06, May 4, 2005 Ubuntu Security Notice, USN-128-1, May 17, 2005 **Turbolinux Security Advisory , TLSA-2005-61, June 1, 2005**
Multiple Vendors Qpopper 4.x; Gentoo Linux	Several vulnerabilities have been reported: a vulnerability was reported because user supplied config and trace files are processed with elevated privileges, which could let a malicious user create/overwrite arbitrary files; and a vulnerability was reported due to an unspecified error which could let a malicious user create group or world-writable files. Upgrades available at: ftp://ftp.qualcomm.com/eudora/servers/unix/popper/old/qpopper4.0.5.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-17.xml Debian: http://security.debian.org/pool/updates/main/q/qpopper/	Qpopper Multiple Insecure File Handling CAN-2005-1151 CAN-2005-1152	Medium	Gentoo Linux Security Advisory GLSA 200505-17, May 23, 2005 Secunia Advisory, SA15475, May 24, 2005 Debian Security Advisories, DSA 728-1 & 728-2, May 25 & 26, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**

	SuSE: **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.			
PostgreSQL PostgreSQL 7.3 through 8.0.2	Two vulnerabilities have been reported: a vulnerability was reported because a remote authenticated malicious user can invoke some client-to-server character set conversion functions and supply specially crafted argument values to potentially execute arbitrary commands; and a remote Denial of Service vulnerability was reported because the 'contrib/tsearch2' module incorrectly declares several functions as returning type 'internal.' Fix available at: http://www.postgresql.org/about/news.315 Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-12.xml Trustix: http://www.trustix.org/errata/2005/0023/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-433.html** Currently we are not aware of any exploits for these vulnerabilities.	PostgreSQL Remote Denial of Service & Arbitrary Code Execution CAN-2005-1409 CAN-2005-1410	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013868, May 3, 2005 Ubuntu Security Notice, USN-118-1, May 04, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-12, May 16, 2005 Trustix Secure Linux Bugfix Advisory, TSL-2005-0023, May 16, 2005 **Turbolinux Security Advisory , TLSA-2005-62, June 1, 2005** **RedHat Security Advisory, RHSA-2005:433-17, June 1, 2005**
Sun Microsystems, Inc. Solaris 10.0	A vulnerability has been reported in the C Library ('libc' and 'libproject') due to an unspecified error, which could let a malicious user obtain elevated privileges. Patch available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101740-1&searchclause=i Currently we are not aware of any exploits for this vulnerability.	Sun Solaris C Library Elevated Privileges CAN-2005-1887	Medium	Sun(sm) Alert Notification, 101740, June 3, 2005
Tomasz Lutelmowski LutelWall 0.97 & prior	A vulnerability has been reported in the 'new_version_check()' function due to the insecure creation of temporary files when updating to a new version, which could let a malicious user obtain root privileges. No workaround or patch available at time of publishing. There is no exploit code required.	LutelWall Insecure Temporary File Creation CAN-2005-1879	High	Security Tracker Alert, 1014112, June 6, 2005
Yapig Yapig 0.92b, 0.93u, 0.94u	Several vulnerabilities have been reported: a vulnerability was reported because it is possible to upload arbitrary files to a directory inside the web root, which could let a remote malicious user execute arbitrary PHP code; a Cross-Site Scripting vulnerability was ported in 'view.php' due to insufficient sanitization of the 'phid' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to insufficient verification of the 'BASE_DIR' and 'YAPIG_PATH' parameters, which could let a remote malicious user include arbitrary files from external and local resources; and a Directory Traversal vulnerability was reported in 'upload.php' due to insufficient verification of the 'dir' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	YaPiG Multiple Vulnerabilities CAN-2005-1881 CAN-2005-1882 CAN-2005-1883 CAN-2005-1884 CAN-2005-1885 CAN-2005-1886	High	SecWatch Advisory, June 4, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
America OnLine Instant Messenger 5.9.3797, 5.5.3595, 5.5.3415 Beta, 5.5, 5.2.3292, 5.1.3036, 5.0.2938	A remote Denial of Service vulnerability has been reported when a malicious user crafts a malformed GIF file that is used as a Buddy Icon and followed by sending an instant message. No workaround or patch available at time of publishing.	AOL Instant Messenger Buddy Icon Remote Denial of Service CAN-2005-1891	Low	Security Focus, 13880, June 7, 2005

	There is no exploit code required.			
AppIndex MWChat 6.x	A vulnerability has been reported because the 'start_lobby.php' script includes the 'chat_maintainance.php' script without validation the '$CONFIG[MWCHAT_Libs]' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AppIndex MWChat Remote Arbitrary Code Execution CAN-2005-1869	High	Security Tracker Alert, 1014090, June 2, 2005
Calendarix Calendarix Advanced 1.5 .20050501	Multiple vulnerabilities have been reported: a vulnerability was reported in 'admin/cal_admintop.php' due to insufficient validation of the 'calpath' parameter, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported due to insufficient sanitization of input passed to the 'catview,' 'id,' and 'year' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. I No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Calendarix Multiple SQL Injection & Cross-Site Scripting CAN-2005-1864 CAN-2005-1865 CAN-2005-1866	High	Security Tracker Alert ID: 1014083, May 31, 2005
Cute PHP Team CuteNews 0.x, 1.x	A vulnerability has been reported due to insufficient sanitization of input when editing template files before used to create templates, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	CuteNews Template Creation Arbitrary PHP Code Execution CAN-2005-1876	High	Secunia Advisory, SA15594, June 3, 2005
Drupal Drupal 4.6, 4.5-4.5.2, Drupal Drupal 4.4-4.4.2	A vulnerability has been reported in the privilege system due to an input validation error, which could let a remote malicious user obtain administrative access. Updates available at: http://drupal.org/project Currently we are not aware of any exploits for this vulnerability.	Drupal Privilege System Administrative Access CAN-2005-1871	High	Drupal Security Advisory, DRUPAL-SA-2005-001, June 2, 2005
Exhibit Engine Exhibit Engine 1.54 RC4, 1.22	An SQL injection vulnerability has been reported in 'List.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Exhibit Engine List.php SQL Injection CAN-2005-1875	High	Security Focus, 13844, June 2, 2005
FlatNuke FlatNuke 2.x	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the 'foot_news.php' script; a vulnerability was reported due to insufficient sanitization of input passed to the 'Referer' HTTP header, which could let a remote malicious user execute arbitrary PHP code; a Cross-Site Scripting vulnerability was reported in 'help.php' and 'footer.php' due to insufficient sanitization of the 'border' and back' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in 'thumb.php' due to insufficient verification of the 'image' parameter before used to view images, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because it is possible to obtain the full path to certain scripts when invalid input is supplied or when they are accessed directly. Updates available at: http://flatnuke.sourceforge.net/index.php?mod=read&id=1117979256 Proofs of Concept exploits have been published.	FlatNuke Multiple Vulnerabilities CAN-2005-1892 CAN-2005-1893 CAN-2005-1894 CAN-2005-1895 CAN-2005-1896	High	SecWatch Advisory, June 6, 2005
Flexcast Streaming Flex Streaming Audio Video Streaming Server 0.1-0.5.1	A vulnerability has been reported in the suppliers and terminal authentication due to an unspecified error. The impact was not specified. Update to version 2.0 or later. Currently we are not aware of any exploits for this vulnerability.	FlexCast Audio Video Streaming Server Terminal Authentication CAN-2005-1897	Not Specified	Secunia Advisory, SA15441, June 6, 2005

Hewlett Packard Company OpenView Radia 3.1.2 .0, 3.1 .0.0	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in the Radia Notify Daemon due to a boundary error in the 'nvd_exec()' function, which could let a remote malicious user execute arbitrary code; and a stack-based buffer overflow vulnerability was reported in the Radia Notify Daemon due to a boundary error when processing command variable extensions, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	HP OpenView Radia Buffer Overflows CAN-2005-1825 CAN-2005-1826	High	Security Tracker Alert, 1014089, June 1, 2005
IBM WebSphere Application Server 5.x	A buffer overflow vulnerability has been reported in the authentication process of the administrative console due to a boundary error, which could let a malicious user execute arbitrary code. Update available at: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24009775 Currently we are not aware of any exploits for this vulnerability.	IBM WebSphere Application Server Administrative Console Buffer Overflow CAN-2005-1872	High	Secunia Advisory, SA15598, June 3, 2005
I-Man I-Man 0.x	A vulnerability has been reported due to an error when handling file attachments, which could let a remote malicious user execute arbitrary PHP code. Upgrade available at: http://prdownloads.sourceforge.net/i-man/i-man-1.0.tar.gz?download There is no exploit code required.	I-Man File Attachments Upload CAN-2005-1868	High	Secunia Advisory, SA15558, June 1, 2005
LPanel LPanel 1.59 & prior	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'diagnose.php' script due to insufficient sanitization of the 'domain' parameter, which could let a remote malicious user reset DNS values; a vulnerability was reported in the 'view_ticket.php' script due to insufficient sanitization of the 'close,' 'pid,' and 'open' parameters, which could let a remote malicious user respond to arbitrary support tickets and execute arbitrary HTML code; a vulnerability was reported in the 'viewreceipt.php' script due to insufficient sanitization of the 'inv' URI parameter, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported in the 'domains.php' script due to insufficient sanitization of the 'editdomain' URI parameter, which could let a remote malicious user change DNS information for arbitrary accounts. No workaround or patch available at time of publishing. There is no exploit code required.	LPanel Multiple Input Validation CAN-2005-1877	High	Security Focus, 13869, June 6, 2005
MediaWiki MediaWiki 1.x	A vulnerability has been reported due to insufficient sanitization of input passed to certain HTML attributes, which could let a remote malicious user execute arbitrary script code. Upgrades available at: http://prdownloads.sf.net/wikipedia/mediawiki-1.4.5.tar.gz?download There is no exploit code required.	MediaWiki Page Template Arbitrary Code Execution CAN-2005-1888	High	Security Focus, 13861, June 6, 2005
Mozilla Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1, 1.0-1.0.3	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of 'IFRAME' JavaScript URLS from being executed in the context of another history list URL, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'InstallTrigger .install()' due to insufficient verification of the 'Icon URL' parameter, which could let a remote malicious user execute arbitrary JavaScript code. Workaround: Disable "tools/options/web-Features/>Allow web sites to install software" Slackware: ftp://ftp.slackware.com/pub/slack ware/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-11.xml	Mozilla Firefox Remote Arbitrary Code Execution CAN-2005-1476 CAN-2005-1477	High	Secunia Advisory, SA15292, May 9, 2005 US-CERT VU#534710 US-CERT VU#648758 Slackware Security Advisory, SSA:2005-135-01, May 15, 2005 Gentoo Linux Security Advisory, GLSA 200505-11, May 16, 2005 Turbolinux Security Advisory, TLSA-2005 -56, May 16, 2005

	TurboLinux: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/m/ mozilla-firefox/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Proofs of Concept exploit scripts have been published.			RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/ products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/ products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/m/ mozilla-firefox/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005 -56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported when processing 'javascript:' URLs, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/ products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/ products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/m/ mozilla-firefox/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE**	Mozilla Suite And Firefox Wrapped 'javascript:' URLs CAN-2005-1531	High	Mozilla Foundation Security Advisory, 2005-43, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 **SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005**

	Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Sun ONE Web Server 6.1, SP1 &SP2; Oracle Oracle9i Application Server Web Cache 9.0.2 .3, 9.0.2 .2; Microsoft IIS 5.0, 6.0 ; IBM Websphere Application Server 5.1.1-5.1.1 .3, 5.1- 5.1 .0.5, 5.0-5.0.2.10; DeleGate DeleGate 8.11, 8.11.1, 8.10-8.10.6, 8.9- 8.9.6; BEA Systems WebLogic Express 8.1 SP 1; Apache Software Foundation Tomcat 5.0.30, 5.0, 4.1.24, Apache 2.0.45-2.0.53, 1.3.29	Multiple vendors are vulnerability to a new class of attack named 'HTTP Request Smuggling' that revolves around piggybacking a HTTP request inside of another HTTP request, which could let a remote malicious user conduct cache poisoning, cross-site scripting, session hijacking and other attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Multiple Vendor Multiple HTTP Request Smuggling	High	Security Focus, 13873, June 6, 2005 Watchfire White Paper, June 6, 2005
Multiple Vendors Gentoo Linux; Dzip Dzip 2.81-2.84, 2.9, 2.8	A Directory Traversal vulnerability has been reported when extracting archives, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200506-03.xml There is no exploit code required.	Dzip Remote Directory Traversal CAN-2005-1874	Medium	Gentoo Linux Security Advisory, GLSA 200506-03, June 6, 2005

Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386 SGI IRIX 6.5.24-6.5.27	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005 SGI Security Advisory, 20050405-01-P, May 26, 2005 **Debian Security Advisory, DSA 731-1, June 2, 2005** **Conectiva Security Advisory, CLSA-2005:962, June 6, 2005**

	SGI: ftp://oss.sgi.com/projects/ sgi_propack/download /3/updates/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/ search/document.do? assetkey=1-26-57761-1 Openwall: http://www.openwall.com/ Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/ elmodocs2/security/ ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/ glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/ document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/ Owl/CHANGES-current.shtml SCO: ftp://ftp.sco.com/pub/updates/ OpenServer/SCOSA-2005.23 SGI IRIX: Apply patch 5892 for IRIX 6.5.24-6.5.27: ftp://patches.sgi.com/ support/free/security/patches/ **Debian:** **http://security.debian.org/ pool/updates/main/k/krb4/** **Conectiva:** **http://distro.conectiva.com.br/ atualizacoes/index.php?id= a&anuncio=000962** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Cisco Systems Cisco Aironet 1200 Series Access Point, 350 Series Access Point, Content Services Switch 11000 Series (WebNS), MGX 8200 Series Edge Concentrators, MGX 8800 Series Multiservice Switches, MGX 8900 Series Multiservice Switches, SN5400 Series Storage Routers; OpenBSD 3.x; Hitachi GR2000 Series Gigabit Routers, GR4000 Series Gigabit Routers, GS3000 Series Gigabit Switches, GS4000 Series Gigabit Switches; ALAXALA Networks AX5400S, AX7800R, AX7800S; FreeBSD FreeBSD 2.x, 3.x, 4.x	A remote Denial of Service vulnerability has been reported in the Protection Against Wrapped Sequence Numbers (PAWS) technique that was included to increase overall TCP performance. Update information available at: http://www.cisco.com/warp/ public/707/cisco-sn- 20050518-tcpts.shtml OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/ patches/3.6/common/015_tcp.patch Hitachi: The vendor has issued updated versions. ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. Microsoft: http://www.microsoft.com/ technet/security/advisory/ 899480.mspx FreeBSD: http://www.freebsd.org/cgi/ cvsweb.cgi/src/sys/netinet/	Cisco Various Products TCP Timestamp Denial of Service CAN-2005-0356	Low	Cisco Security Notice, 64909, May 18, 2005 Microsoft Security Advisory (899480), May 18, 2005 **US-CERT VU#637934** FreeBSD CVS Log, May 25, 2005

	tcp_input.c An exploit script has been published.			
Multiple Vendors MandrakeSoft Linux Mandrake 10.2 X86_64, 10.2; Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75, 0.78, 0.82, 0.82.1, 1.0-1.0.2, 1.1.1-1.1.4, 1.2, 1.2.1; Ubuntu Linux 4.1 ppc, ia64, ia32, 5.0 4 powerpc, i386, amd64	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported when handling long URIs due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereference error when handling MSN messages. Rob Flynn: http://prdownloads.sourceforge.net/gaim/gaim-1.3.0.tar.gz?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-429.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-09.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000964** A Proof of Concept exploit script has been published.	Gaim Remote Buffer Overflow & Denial of Service CAN-2005-1261 CAN-2005-1262	Low/ High (High if arbitrary code can be executed)	Fedora Update Notification, FEDORA-2005-369, May 11, 2005 RedHat Security Advisory, RHSA-2005:429-06, May 11, 2005 Gentoo Linux Security Advisory, GLSA 200505-09, May 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:086, May 12, 2005 Ubuntu Security Notice, USN-125-1, May 12, 2005 **Conectiva Security Advisory, CLSA-2005:964, June 7, 2005**

PHP Group PHP prior to 5.0.4; Peachtree Linux release 1	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ Debian: http://security.debian.org/pool/updates/main/p/php4/ **Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory, DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Debian Security Advisory, DSA 729-1, May 26, 2005 **Conectiva Security Advisory, CLSA-2005:955, May 31, 2005**
phpBB Group phpBB 2.0.15	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of BBCode URL tags, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	phpBB BBCode URL Tag Cross-Site Scripting	High	Security Tracker Alert, 1014117, June 7, 2005
phpCMS phpCMS1.2.0, 1.2.1, pl1	A vulnerability has been reported in the 'class.layour_phpcms.php' source file, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.phpcms.de/download/index.en.html A Proof of Concept exploit has been published.	phpCMS Information Disclosure CAN-2005-1840	Medium	Security Focus, 13843, June 2, 2005
phpThumb phpThumb 1.5-1.5.3	A vulnerability has been reported in 'phpThumb.php' due to insufficient sanitization of the 'src' parameter, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/phpthumb/phpThumb_1.5.4.zip?download Currently we are not aware of any exploits for this vulnerability.	PHPThumb Arbitrary File Information Disclosure CAN-2005-1898	Medium	Security Focus, 13842, June 2, 2005

Popper Popper 1.41 -r2	A vulnerability has been reported in 'childwindow.inc.php' due to insufficient verification of the 'form' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Popper Webmail 'ChildWindow.Inc.PHP' Remote Arbitrary Code Execution CAN-2005-1870	High	LSS Security Advisory, LSS-2005-06-07, June 1, 2005
PortailPHP PortailPHP 1.3	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. **An exploit script has been published.**	PortailPHP ID Parameter SQL Injection CAN-2005-1701	High	Security Focus, 13708, May 23, 2005 **Security Focus, 13708, June 7,2005**
Rakkarsoft L.L.C. Rakkarsoft Raknet 2.33; nFusion Interactive Elite Warriors: Vietnam 1.3	A remote Denial of Service vulnerability has been reported when handling an empty UDP packet. The vulnerability has been fixed in an updated 2.33 version (after 2005-05-30). A Proof of Concept exploit has been published.	Rakkarsoft RakNet Remote Denial of Service CAN-2005-1899	Low	Security Focus, 13862, June 6, 2005
Sawmill Sawmill 7.0.x, 7.1-7.1.5	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error, which could let a remote malicious user obtain administrative access; a vulnerability was reported due to an unspecified error which could let a remote malicious user add a license without being authenticated; and a Cross-Site Scripting vulnerability was reported in the 'Add User' window due to insufficient sanitization of the username and in the licensing page due to insufficient sanitization of the license key, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.sawmill.net/downloads.html There is no exploit code required.	Sawmill Elevated Privileges & Cross-Site Scripting CAN-2005-1900 CAN-2005-1901	High	Secunia Advisory, SA15499, June 6, 2005
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Apple: http://www.apple.com/support/downloads/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://www.debian.org/security/2005/dsa-662 Red Hat: http://rhn.redhat.com/errata/RHSA-2005-135.html Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/ Fedora: http://download.fedora.redhat.	SquirrelMail Cross-Site Scripting CAN-2004-1036 CAN-2005-0104 CAN-2005-0152	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004 Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Debian DSA-662-1, February 1, 2005 Red Hat RHSA-2005:135-04, February 10, 2005 Debian Security Advisory, DSA 662-2, March 14, 2005 Fedora Update Notifications FEDORA-2005-259 & 260, March 28, 2005 **SUSE Security Summary Report,**

	com/pub/fedora/linux/core/updates/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** An exploit script is not required.			**SUSE-SR:2005:014, June 7, 2005**
Sun Microsystems, Inc. Sun ONE Application Server 6.x	A vulnerability has been reported due to an unspecified error, which could let a remote malicious user obtain sensitive information. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101690-1 Currently we are not aware of any exploits for this vulnerability.	Sun One Application Server File Disclosure CAN-2005-1889	Medium	Sun(sm) Alert Notification, 101690, June 6, 2005
Symantec Brightmail Anti-Spam 6.0.1, 6.0, 5.5, 4.0	A vulnerability has been reported due to a static database administration password, which could let a remote malicious user obtain administrative access to the quarantined message database. Updates available at: http://www.symantec.com/techsupp/ There is no exploit code required.	Symantec Brightmail AntiSpam Remote Information Disclosure CAN-2005-1867	High	Symantec Security Advisory, SYM05-009, May 31, 2005
WordPress WordPress 1.5, 1.5.1	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'cat_ID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://wordpress.org/latest.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200506-04.xml** **An exploit script has been published.**	Wordpress Cat_ID Parameter SQL Injection CAN-2005-1810	High	Secunia Advisory, SA15517, May 30, 2005 **Gentoo Linux Security Advisory, GLSA 200506-04, June 6, 2005**

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Bluetooth Security Review, Part 2:** Article that looks at Bluetooth viruses, several unpublished vulnerabilities in Symbian based phones, and then discusses "Blue tag" tracking, positioning, and privacy issues. Source: http://www.securityfocus.com/infocus/1836.
- **Bluetooth Security Review, Part 1:** An introduction to Bluetooth and some of its security and privacy issues, including how it is detected and some implementation issues from various mobile phone vendors. Source: http://www.securityfocus.com/infocus/1830

Wireless Vulnerabilities

- **New hack cracks 'secure' Bluetooth devices:** A paper that describes a vulnerability that exists in the device pairing process has been published. It describes a passive attack which could let a remote malicious user find the PIN used during the pairing process. Source: http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/.
- **Linux Kernel Bluetooth Signed Buffer Index vulnerability** (For more information, see entry in the Multiple Operating Systems Table)
- **Yamaha MusicCAST MCX-1000 wireless network interface:** The Yamaha MusicCAST MCX-1000 server wireless networking interface is enabled by default, cannot be disabled, and operates in Access Point mode, which could let a remote malicious user access the MusicCAST wireless network and potentially any other network connected to the MusicCAST. Source: US-CERT VU#758582.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Bluetooth Security Review, Part 2Script name	Workaround or Patch Available	Script Description
June 7, 2005	portailphp-sql-inj.pl	No	Exploit for the PortailPHP ID Parameter SQL Injection vulnerability.
June 7, 2005	wordpress-sql-inj.pl	Yes	Exploit for the Wordpress Cat_ID Parameter SQL Injection vulnerability.
June 6, 2005	memfs.c	Yes	Proof of Concept exploit for the FUSE Information Disclosure vulnerability.

June 6, 2005	rakzero.zip	Yes	Exploit for the Rakkarsoft RakNet Remote Denial of Service vulnerability.
June 6, 2005	webapp-poc.sh.txt	Yes	Proof of Concept exploit for the Gentoo webapp-config Insecure Temporary File vulnerability.
June 3, 2005	crob_RMD_overflow.c	No	Proof of Concept exploit for the Crob FTP Server Remote RMD Command Stack Buffer Overflow vulnerability.
June 2, 2005	globalscapeftp_user_input.pm	Yes	Proofs of Concept exploits for the GlobalSCAPE Secure FTP Server Remote Buffer Overflow vulnerability.
June 2, 2005	Mezcal	NA	An HTTP/HTTPS brute forcing tool that allows the crafting of requests and insertion of dynamic variables on-the-fly.
June 1, 2005	ettercap-NG-0.7.3.tar.gz	N/A	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
June 1, 2005	framework-2.4.tar.gz	N/A	The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code.
June 1, 2005	MS05-021-PoC.pl	Yes	Exploit for the Microsoft Exchange Server Remote Code Execution Vulnerability.
June 1, 2005	ret-onto-ret_en.txt	N/A	Whitepaper that discusses how Linux 2.6.x vsyscalls may be used as powerful attack vectors.
June 1, 2005	spapromailExp.cpp	Yes	Proof of Concept exploit for the SPA-PRO Mail @Solomon IMAP Server Buffer Overflow Vulnerability.
June 1, 2005	vr-9.3c.tar.gz	N/A	A traceroute tool that displays a map of the path to the destination server by looking up the geographical location of each traceroute hop.
June 1, 2005	yersinia-0.5.4.tar.gz	N/A	Yersinia implements several attacks for the following protocols: Spanning Tree (STP), Cisco Discovery (CDP), Dynamic Host Configuration (DHCP), Hot Standby Router (HSRP), Dynamic Trunking (DTP), 802.1q and VLAN Trunking (VTP), helping a pen-tester with different tasks.

[back to top]

Trends

- **Pharming for profits:** According to a workshop at the InBox e-mail security conference, an increase in pharming attacks has produced a steep rise in cybercrime statistics. Hackers today are committing fraud at alarming rates, using sophisticated, multilayered "pharming" botnets that point to the need for new forms of authentication to secure e-mail originators as well as Web site destinations. Analysis shows that 54% of all malware is designed to harvest confidential information from users, up from 44% in the second half of 2004 and 36% in the first half. Source: http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,102179,00.html
- **Custom worms built for industrial espionage**: The industrial espionage ring broken by Israeli police last week, where private investigators hired a programmer to custom create a Trojan horse that was then planted on rivals' PCs, is only the most recent evidence of a trend towards smart targeting by hackers. Source: http://www.securitypipeline.com/news/163702820
- **"Remarkably sophisticated" web attack detailed**: A new "remarkably sophisticated" attack that uses three pieces of malware to turn PCs into zombies that can be sold to criminal groups appeared on the Internet this week, security vendor Computer Associates International Inc. said yesterday. A version of the Bagle worm downloader that the company has dubbed Glieder is serving as a "beachhead" to install more serious malware on computers, CA said. Demonstrating a new level of coordination between Glieder and other attacks, infected computers can have their antivirus and firewall software disabled and can be turned into remotely controlled zombies used to mount large cyberattacks, CA said. Source: http://www.computerworld.com/securitytopics/security/story/0,10801,102214,00.html

[back to top]

Viruses/Trojans

Recent Threats

- **Bagle**: At least three new versions of the Bagle e-mail worm are spreading quickly on the Internet, according to several Internet security firms. About 80 variants of the original Bagle worm, which first appeared in January 2004, have been released on the Internet. Damage from the new Bagle variants should be minor as antivirus vendors are reacting quickly to the attacks. The first two variants were tentatively dubbed Bagle.CA and Bagle.CB, which would make them the 79th and 80th Bagle variants. Source: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,102143,00.html
- **Mytob**: Dubbed "Mytob.bi," this variant of Mytob scans the hard drive of an infected machine and sends copies of itself to email addresses it finds in the Windows Address Book. The worm poses as a message from an IT administrator, warning recipients that their email account is about to be suspended, Trend Micro said. Source: http://www.techworld.com/security/news/index.cfm?NewsID=3772 Virus writers responsible for the recent rash of Mytob worm variants could be working on creating a superworm, a security researcher also warned. The HellBot group behind the Mytob worms writes programming instructions in its code that mirror the way developers work, said Sophos PLC security consultant Carole Theriault. "The only conclusion we can come up with is that they are working on a big superworm," she said. Source: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,102220,00.html

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Mytob.C	Win32 Worm	Increase	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
2	Netsky-P	Win32 Worm	Slight Decrease	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
3	Netsky-Q	Win32 Worm	Slight Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
4	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
5	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
6	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
7	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
8	Netsky-Z	Win32 Worm	Slight Decrease	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
9	Netsky-B	Win32 Worm	Stable	February 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. Also searches drives for certain folder names and then copies itself to those folders.
10	MyDoom-O	Win32 Worm	Stable	July 2004	A mass-mailing worm that uses its own SMTP engine to generate email messages. It gathers its target email addresses from files with certain extension names. It also avoids sending email messages to email addresses that contain certain strings.

Table Updated June 7, 2005

[back to top]

Last updated June 08, 2005